WE CLAIM:

1. A secure data switching node comprising:

   a. a plurality of communications ports;

   b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

   c. a plurality of switching entry protection flags, each one of the plurality of switching entry protection flags being associated with a switching entry; and

   d. a controller executing a secure switching database update process,

   whereby an attempt by a hostile data network node to effect a modification of a protected switching entry is prevented when the protection flag is set, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

2. A secure data switching node as claimed in claim 1, wherein the communication ports are represented in the switching entries via port identifiers.

3. A secure data switching node comprising:

   a. a plurality of physical communications ports;

   b. a switching database having a plurality of switching entries, each one of the plurality of switching

entries specifying an association between a data network node identifier and a communications port;

c. a plurality of topology discovery disable flags, each one of the plurality of topology discovery disable flags being associated with a communications port; and

d. a controller executing a secure data transport network topology update process

whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port associated with a topology discovery disabled physical communications port are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

4. A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

c. a plurality of topology discovery disable flags, each one of the plurality of topology discovery disable flags being associated with a communications port;

d. a global unknown destination flood control flag; and

e. a controller implementing a secure Payload Data Unit (PDU) forwarding process

whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

5. A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

c. a plurality of unknown destination flood control flags, each one of the plurality of unknown destination flood control flags being associated with a communications port; and

d. a controller implementing a secure Payload Data Unit (PDU) forwarding process

whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

6. A method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of:

   a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

   b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key;

   c. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database; and

   d. modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset

   whereby preventing a redirection of data traffic processed by the data switching node.

7. A method of securely updating data transport network topology information of a held in a switching database of a data switching node associated with the data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key; and

c. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database and an associated topology discovery disable flag is reset

whereby a hostile data network node is prevented from connecting to the source physical communications port.

8. A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with the source communications port.

9. A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with all physical communications ports of the data switching node.

10. A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key;

c. replicating the received data traffic to each one of a plurality of physical communications ports of the data switching node if a global unknown destination flood control flag associated with the data switching node is reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set if the global unknown destination flood control flag is set

whereby a hostile data network node connected to a physical communications port having the topology discovery disable flag set is prevented from spying on unknown destination data traffic.

11. A method as claimed in claim 10, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replications of the data traffic to the source communications port.

12. A method as claimed in claim 10, wherein each physical communications port further includes an associated unknown destination flood control bit, the method further comprising a step of: suppressing the replication of the data traffic to communications ports having the associated unknown destination flood control bit set.

13. A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key;

c. replicating the received data traffic to each one of a plurality of communications ports of the data switching node if an unknown destination flood control flags associated with the physical communications ports are reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having the unknown destination flood control flag set.

whereby a hostile data network node connected to a physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic.

14. A method as claimed in claim 13, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replication of the data traffic to the source communications port.